UNITED STATES PATENT AND TRADEMARK OFFICE

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/851,745	05/09/2001	William Rex Akers	HTHC 3423000	3915

21909   7590   12/10/2009

CARR LLP
670 FOUNDERS SQUARE
900 JACKSON STREET
DALLAS, TX 75202

EXAMINER
MORGAN, ROBERT W

ART UNIT	PAPER NUMBER
3626	

MAIL DATE	DELIVERY MODE
12/10/2009	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.
- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *06 July 2009*.
2a)☐ This action is **FINAL**.   2b)☒ This action is non-final.
3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-36* is/are pending in the application.
   4a) Of the above claim(s) _____ is/are withdrawn from consideration.
5)☐ Claim(s) _____ is/are allowed.
6)☒ Claim(s) *1-36* is/are rejected.
7)☐ Claim(s) _____ is/are objected to.
8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.
10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.
   Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
   Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
   a)☐ All   b)☐ Some * c)☐ None of:
   1.☐ Certified copies of the priority documents have been received.
   2.☐ Certified copies of the priority documents have been received in Application No. _____.
   3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).
   * See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)
1) ☐ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO/SB/08)
   Paper No(s)/Mail Date *7/28/09*.
4) ☐ Interview Summary (PTO-413)
   Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

Continued Examination Under 37 CFR 1.114

1.   A request for continued examination under 37 CFR 1.114, including the fee set forth in

37 CFR 1.17(e), was filed in this application after final rejection. Since this application is

eligible for continued examination under 37 CFR 1.114, and the fee set forth in 37 CFR 1.17(e)

has been timely paid, the finality of the previous Office action has been withdrawn pursuant to

37 CFR 1.114. Applicant's submission filed on 7/28/09 has been entered.

Notice to Applicant

2.   This communication is in response to the amendment filed 7/28/09, the following has

occurred: claims 1, 3, 7, 9-13, 15-17, 20, 23-24, 27, and 29 have been amended and claim 36 has

been added. Claims 1-36 are presented for examination.

Information Disclosure Statement

3.   The information disclosure statement filed on 7/28/09 has been acknowledged and

entered.

Claim Rejections - 35 USC § 103

4.   The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all

obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in
> section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are
> such that the subject matter as a whole would have been obvious at the time the invention was made to a person
> having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the
> manner in which the invention was made.

Claims 1-15, 23-24, 27-31 and 33 are rejected under 35 U.S.C. 103(a) as being

unpatentable over U.S. Patent No. 5,924,074 to Evans in view of U.S. Patent No. 7,251,610 to

Alban et al., U.S. Patent No. 7,027,872 to Thompson and U.S. Patent No. 7,039,810 to Nichols

As per claim 1, Evans teaches electronic medical record system that includes a server

(406, Fig. 24) connected to client machines running application such as Microsoft Windows to

access the data (see: column 14, lines 8-16). Evans further teaches an electronic medical record

system including servers (406, Fig. 24) that allow patient data to be transfer between external

sources as well as updating the patient record (reads on "transmit the first version of the medical

record data file to the record client") (see: column 3, lines 37-43 and column 5, lines 36-40).

Evans fails to teach:

--the claimed wherein encapsulation the portion of the medical record file comprises

generating a value based on the data structure of the medical record data file;

 --the claimed encrypting the first version of the medical record data file;

--the claimed receive a received version of the medical record data file from the record

client, the received version having additional data added to the medical record data file;

--the claimed file detection system configured to detect, based on the value, if the sealed

medical data has been modified from the first version in the received version;

--the claimed record database system configured to, if the sealed medical data has been

modified from the first version in the received version, store the sealed medical data in the first

version separately from the modifications; and

--the claimed notification system configured to, if the sealed medical data has been modified from the first version in the received version, generate notification data comprising notification of the modifications.

Alban et al. teaches a clinical documentation system for multiple caregivers with a user interface that allow a caregiver to quickly identify and review clinically appropriate information for a given situation. Alban also teaches that the user interface allows caregivers to file a note (to store in on the server) as well as take appropriate follow up actions for specific entries in a patient's acute care record, for example, for a supervising physician to review document, and cosign an entry made by a resident (see: column 3, lines 34-56). In addition, Alban et al. teaches a filter function allows the user to modify the types of notes that appear in the notes listing window, for example, notes may be filtered by time, author type, author, medical service, etc. (see: column 6, lines 3-13).

One of ordinary skill in the art at the time the invention was made would have found it obvious to include a clinical documentation system for multiple caregivers as taught by Alban et al. within the system as taught by Evans with the motivation of providing a means for a user to quickly see information that's been added to the patient's record since the user's last review (see: Alban et al.; column 1, lines 62-64).

Evans and Alban et al. fail to teach:

--the claimed wherein encapsulation the portion of the medical record file comprises generating a value based on the data structure of the medical record data file; and

--the claimed file detection system configured to detect, based on the value, if the sealed medical data has been modified from the first version in the received version.

Thompson teaches variable encryption scheme for data transfer including encrypting

patient data according to the sensitive of data and default values (see: column 5, lines 58 to

column 6, lines 11). In addition, Thompson teaches that medical data can be transferred across

various storage, memory and server platforms (see: column 4, lines 23-26).

Therefore, it would have been obvious to a person of ordinary skill in the art at the time

the invention was made to include generating values to encrypted/encapsulated medical file as

taught by Thompson within the electronic medical record system as taught by Evans with the

motivation of protecting privacy and ensuring data authenticity (see: Thompson: column 2, lines

39-40).

Evans, Alban et al. and Thompson fail to teach the claimed encrypting the first version of

the medical record data file.

Nichols teaches that sensitive data such as patient records are securely transferred

between a programmer and a data encryption (see: abstract). In addition, Nichols teaches that

before sensitive information (221, Fig. 5) is transmitted across data communication media (226,

Fig. 5) it is encrypted by encryption engine (230, Fig. 5) (see: column 15, lines 9-15). Data

encryption has been increasingly used to add security and privacy to data, voice and video

transmissions across public networks (see: column 2, lines 54-56). The Examiner considers the

data to be automatically encrypted and preserved before transmission.

Therefore, it would have been obvious to a person of ordinary skill in the art at the time

the invention was made to include encryption of medical information as taught by Nichols with

as taught by Evans and Thompson with the motivation of providing an apparatus and method for

securely transferring sensitive information, such as patient information using encryption methods to prevent abuse (see: Nichols: column 1, lines 19-24).

As per claim 2, Evans teaches the claimed record server further comprises a sync system configured to verify that the record client has received a sync file before transferring the medical record data file. This feature is met by the electronic medical record system including web servers (406, Fig. 24) that allow patient data to be transfer between external source as well as updating the patient record obviously suggesting that the comparing and checking of medical data take place to verify that an up-to-date medical record is available (see: column 3, lines 37-43 and column 5, lines 36-40).

As per claim 3, Evans teaches the claimed record server further comprises a tracking system updating configured to update a tracking record when the received version of the medical record data file is received by the record server. This feature is met by the tracking and description of patient data within the system (see: column 9, lines 27-37).

As per claim 4, Evans teaches the claimed record client further comprises a tracking system configured to update a tracking record when the medical record data file is accessed. This limitation is met by the electronic medical record system which updates patient's records upon a nurses or physician entry of information into the system (see: column 5, lines 29-40).

As per claim 5, Evans teaches the claimed record client further comprises a remote data system configured to generate medical record data. This limitation is met by the electronic medical record system that includes server (406 Fig. 24) that are connected to client machines running application such as Microsoft Windows to access and generating medical data (see: column 14, lines 8-16).

As per claim 6, Evans teaches an electronic medical record system that transfers patient data from the electronic medical records system to other healthcare providers and between external sources (see: column 3, lines 36-42 and column 4, lines 64 to column 5, lines 8). In addition, Evans teaches the use of progress notes (144, Fig. 4) to summarize details of the patient's condition and to review the patient's progress over time (see: column 6, lines 31-36).

Evans fails to teach record client system further comprises a detail encapsulation system configured to receive comment data and encapsulate the comment data.

Nichols teaches that sensitive data such as patient records are securely transferred between a programmer and a data encryption (see: abstract). In addition, Nichols teaches that before sensitive information (221, Fig. 5) is transmitted across data communication media (226, Fig. 5) it is encrypted by encryption engine (230, Fig. 5) (see: column 15, lines 9-15).

The obviousness of combining the teachings of Nichols with the system as taught by Evans is discussed in the rejection of claim 1, and incorporated herein.

As per claim 7, Evans teaches the claimed record database system is configured to store at least one version of the medical record data file. This limitation is met by the teaching of Evans of organizing and storing of patient medical records in which are made available for access by authorized personnel (see: column 2, lines 65 to column 3, lines 3).

As per claim 8, Evans teaches the claimed record database system is configured to receive medical record excerpt data and transfer it to a predetermined recipient. This feature is met by the transferred patient data from the electronic medical records system to other healthcare providers (see: column 4, lines 64 to column 5, lines 8).

As per claim 9, Albans et al. teaches the claimed wherein the notification system configured to transfer notification data to a party regarding the availability of medical record data, the notification data comprising notification of the transmission of the first version of the medical record data file to the record client (see: column 4, lines 25-36).

As per claim 10, Evans teaches the claimed a method for transferring electronic medical files comprising:

--the claimed assembling at least the sealed medical record data into a first version of a medical record data file is met by the storing and organizing of patient records in a patient repository (see: column 3, lines 9-16);

--the claimed receiving a request to transfer the medical record data file is met by the point of care system issuing a request to transfer patient data (see: column 9, lines 39-53); and

--the claimed transferring the first version medical record data file to a remote location is met by the transferring of patient data between external sources (see: column 3, lines 36-42).

Evans teaches electronic medical record system that includes a server (406, Fig. 24) connected to client machines running application such as Microsoft Windows to access the data (see: column 14, lines 8-16). Evans further teaches an electronic medical record system including servers (406, Fig. 24) that allow patient data to be transfer between external sources as well as updating the patient record (see: column 3, lines 37-43 and column 5, lines 36-40).

Evans fails to teach:

--the claimed encapsulating sealed medical record data, wherein encapsulating the sealed medical record data comprises generating a value based on the data structure of the sealed medical record data; and

--the claimed encrypting the sealed medical record data;

--the claimed receiving a received version of the medical record data file from the remote

location, the received version having additional data added to the medical record data file;

--the claimed detecting, based on the value, if the sealed medical record data has been

modified from the first version in the received version; and

--the claimed if the sealed medical record data has been modified from the first version in

the received version;

--the claimed storing the sealed medical record data in the first version separately from

the modifications; and

--the claimed generating notification data comprising notification of the modifications.

Alban et al. teaches a clinical documentation system for multiple caregivers with a user

interface that allow a caregiver to quickly identify and review clinically appropriate information

for a given situation. Alban also teaches that the user interface allows caregivers to file a note (to

store in on the server) as well as take appropriate follow up actions for specific entries in a

patient's acute care record, for example, for a supervising physician to review document, and

cosign an entry made by a resident (see: column 3, lines 34-56). In addition, Alban et al. teaches

a filter function allows the user to modify the types of notes that appear in the notes listing

window, for example, notes may be filtered by time, author type, author, medical service, etc.

(see: column 6, lines 3-13).

The obviousness of combining the teachings of Alban et al. within the system as taught

by Evans is discussed in the rejection of claim 1, and incorporated herein.

Evan and Alban et al. fail to teach:

--the claimed encrypting the sealed medical record data; and

--the claimed detecting, based on the value, if the sealed medical record data has been modified from the first version in the received version;

Thompson teaches variable encryption scheme for data transfer including encrypting patient data according to the sensitive of data and default values (see: column 5, lines 58 to column 6, lines 11). In addition, Thompson teaches that medical data can be transferred across various storage, memory and server platforms (see: column 4, lines 23-26).

The obviousness of combining the teachings of Thompson within the system as taught by Evans and Alban et al. are discussed in the rejection of claim 1, and incorporated herein.

Evans, Alban et al. and Thompson fail to teach the claimed encrypting the sealed medical record data.

Nichols teaches that sensitive data such as patient records are securely transferred between a programmer and a data encryption (see: abstract). In addition, Nichols teaches that before sensitive information (221, Fig. 5) is transmitted across data communication media (226, Fig. 5) it is encrypted by encryption engine (230, Fig. 5) (see: column 15, lines 9-15).

The obviousness of combining the teachings of Nichols with the system as taught by Evans is discussed in the rejection of claim 1, and incorporated herein.

As per claim 11, Evans teaches the claimed transferring the first version of the medical record data file to further comprises transferring a sync file to the remote location. This limitation is met by the transferring of patient data between external sources (see: column 3, lines 36-42).

As per claim 12, Evans teaches the claimed assembling the first medical record data into the first medical record data file comprises storing a tracking record with the medical record data file. This feature is met by the electronic medical record system which stores and updates patient records upon a nurses or physician entry of information (see: column 3, lines 9-16 and column 5, lines 29-40).

As per claim 13, Alban et al. teaches the claimed generating notification data at the remote location; the notification data comprising notification of the transfer of the first version of the medical record data file the remote location (see: column 4, lines 25-36) .

As per claim 14, Evans teaches the claimed accessing the medical record data file at the remote location (see: column 2, lines 45-47); and

--the claimed updating a tracking record to show that the medical record data file has been accessed at the remote location is met by the electronic medical record system which allows nurses and physician to access and update patient's records upon entry into the system (see: column 5, lines 29-40).

As per claim 15, Evans teaches:

--the claimed receiving the additional medical record data at the remote location (see: column 10, lines 18-23); and

--the claimed updating the medical record data file to include the additional medical record data is met by the electronic medical record system which allows nurses and physician to access and update patient's records upon entry into the system (see: column 5, lines 29-40).

Evans fails to teach:

--the claimed encapsulating the additional medical record data, wherein encapsulating the additional medical data comprises generating a second value based on the data structure of the additional medical record data file.

Thompson teaches variable encryption scheme for data transfer including encrypting patient data according to the sensitive of data and default values (see: column 5, lines 58 to column 6, lines 11). In addition, Thompson teaches that medical data can be transferred across various storage, memory and server platforms (see: column 4, lines 23-26).

The obviousness of combining the teachings of Thompson within the system as taught by Evans is discussed in the rejection of claim 1, and incorporated herein.

As per claim 23, it is rejected for the same reason given in claims 1 and 10. In addition, Alban et al. teaches that the system (10, Fig. 1) checks the user's security record for authorized activities, and displays the authorized activities in the activity bar (28, Fig. 2) at block (703, Fig. 7) (reads on "sync system) (see: column 6, lines 47-50).

As per claims 24, 27 and 29, they are rejected for the same reason given in claims 1 and 10.

As per claim 28, Evans teaches an electronic medical record system that transfers patient data from the electronic medical records system to other healthcare providers and between external sources (see: column 3, lines 36-42 and column 4, lines 64 to column 5, lines 8).

Evans fails to explicitly teach extracting an excerpt of the electronic medical record data from the electronic medical record data file comprises removing user readable patient identifying data.

Nichols teaches that sensitive data such as patient records are securely transferred

between a programmer and data encryption (see: abstract). In addition, Nichols teaches that

before sensitive information (221, Fig. 5) is transmitted across data communication media (226,

Fig. 5) it is encrypted by an encryption engine (230, Fig. 5) (see: column 15, lines 9-15). The

Examiner considers the encrypting of the patient records to include removing user readable

patient identifying data to protect confidentiality of patient's medical information.

The obviousness of combining the teaching of Nichols and Evans are discussed in the

rejection of claim 1, and incorporated herein.

As per claim 30, Evans teaches the claimed electronic medical record file is comprises an

image data file. This limitation is met by the patient data structure (210, Fig. 13) that maintain a

pointer to a legacy files structure (219, Fig. 13) having patient data transmitted from the legacy

data system (106, Fig. 1), such as an image of a patient chart (see: column 8, lines 57-60).

 As per claim 31, Evans teaches the claimed sync file is comprises a patient file. This

feature is met by the electronic medical record system including web servers (406, Fig. 24) that

allow patient data to be transfer between external sources as well as updating the patient record

(see: column 3, lines 37-43 and column 5, lines 36-40). The Examiner considers the updated

patient record to be the sync file, which is already compared and checked to verify the

availability of an up-to-date medical record.

As per claim 33, Evans teaches the claimed transferring the sync file comprises creating a

patient folder. The limitation is met by the transferring of patient between external sources (see:

column 3, lines 36-42). The Examiner considers the transferring of the patient record (sync file)

to be creating a patient folder one the information is received at a remote location.

5.   Claims 16-17, 19, 35 and 36 are rejected under 35 U.S.C. 103(a) as being unpatentable

over U.S. Patent No. 5,924,074 to Evans in view of U.S. Patent No. 6,305,377 to Portwood et al.

As per claim 16, Evans teaches the claimed record server and record client coupled to the

record server (see: column 14, lines 8-16).

Evans fails to teach a system for distributing packaged medical supplies comprising:

--the claimed generate medical supply package data, the medical supply package data

comprising:

--the claimed identification of at least one physical package containing physical medical

supplies;

--the claimed identification of the physical medical supplies; and

--the claimed identification of a remote site the physical package is to be physically

moved to;

--the claimed transmit the medical supply package data to a record client located at the

remote site; and

--the correlate the package with verification data received from the record client;

--the verification data comprising:

--the claimed identification of at least one physical package received by the record client;

--the claimed identification of a patient prescription received by the record client; and

--the identification of the site of the record client.

Portwood et al. teach a prescription distribution system including a server computer

communicating with other prescriber computer to transfer prescription data to the server for

validation, certification, and distribution (see: abstract, column 3, lines 43-49, column 5, lines 7-

10 and column 7, lines 35-37). In addition, Portwood et al. teaches that prescription can be

distributed to a prescription distribution company, such as a pharmacy, or drug wholesale

company, and in turn the distribution can, via the server, invoice the payor (see: column 7, lines

42-45). The Examiner considers the invoice to contain patient identification information and site

information.

Therefore, it would have been obvious to one having ordinary skill in the art at the time

of the invention to include the prescription distribution system as taught by Portwood et al. with

the electronic medical record system as taught by Evans with the motivation of streamlining and

incorporating automatic mail ordering, billing, and other business aspects, such as prescription

verification and delivery (see: Portwood et al. column 2, lines 9-13).

As per claim 17, Evans teaches the claimed an inventory tracking system coupled to the

record client and configured to update inventory data, the inventory data comprising the size of

an inventory of the physical medical supplies stored at the remote site. This limitation is met by

the tracking system that includes tracking and description of patient data within the system (see:

column 9, lines 27-37). In addition, Evans teaches that the electronic medical record system

updates patient's records upon a nurses or physician entry of information into the system (see:

column 5, lines 29-40). Furthermore, Evans teaches a record server and record client coupled to

the record server (see: Evans: column 14, lines 8-16).

As per claim 19, Evans teaches the claimed record client further comprises a remote data

system, the remote data system configured to generate counseling data and transmit the

counseling data to the record server. This limitation is met by access of the patient record from

any geographical location as well as providing prescription instruction to a patient's record (see: column 2, lines 45-58).

As per claim 35, Evans teaches the record client further comprises an image data capture device configured to generate image data, and wherein the verification data includes comprises the image data. This feature is met by the data source (370, Fig. 23) that comprises physical data (374, Fig. 23) such as paper based records and photographs, and electronic mainframe data (376, Fig. 24). The converter (372, Fig. 24) receives information from the data source (370, Fig. 24) and transforms the information into an electronic format compatible with the EMR system. For example, to input physical data (374, Fig. 24) such as paper or image based data, into a patient record, the converter (372, Fig. 24) comprises a scanner to digitize the physical data into a binary file format for incorporation into the patient's record (see: column 12, lines 35-46).

As per claim 36, Portwood teaches the claimed wherein the physical medical supplies comprise medicine is met by prescription distribution system that enables quicker delivery of prescription at the patient's location (see: abstract and column 5, lines 7-10).

6.   Claim 18 is rejected under 35 U.S.C. 103(a) as being unpatentable over U.S. Patent No. 5,924,074 to Evans and U.S. Patent No. 6,305,377 to Portwood et al. as applied to claim 16 above, and further in view of U.S. Patent No. 7,039,810 to Nichols.

As per claim 18, Evans in combination with Portwood et al. teaches a system with a record server that verifies the data in a medical record data file.

However, Evans in combination with Portwood et al. fails to teach the encapsulating of the verification data.

Nichols teaches that sensitive data such as patient records are securely transferred between a programmer and a data encryption (see: abstract). In addition, Nichols teaches that before sensitive information (221, Fig. 5) is transmitted across data communication media (226, Fig. 5) it is encrypted by encryption engine (230, Fig. 5) (see: column 15, lines 9-15). Additionally, Nichols teaches that a remote data center (224, Fig. 5) receives encrypted sensitive information (221, Fig. 5) transmitted by programmer (222, Fig. 5) and decrypts the encrypted sensitive information (221, Fig. 5). Data encryption has been increasingly used to add security and privacy to data, voice and video transmission across public networks (see: column 2, lines 54-56).

One of ordinary skill in the art at the time the invention was made would have found it obvious to include encryption of medical information as taught by Nichols within the combination of the electronic medical record system as taught by Evans and the prescription distribution system as taught by Portwood et al. with the motivation of providing an apparatus and method for securely transferring sensitive information such as patient information using encryption methods to prevent abuse (see: Nichols: column 1, lines 19-24).

7.   Claims 20-22 are rejected under 35 U.S.C. 103(a) as being unpatentable over U.S. Patent No. 6,305,377 to Portwood et al. in view of U.S. Patent No. 5,924,074 to Evans.

As per claim 20, Portwood et al. teaches a method for distributing packaged medical supplies comprising:

        --the claimed storing package data comprising:

        --the identification of at least one physical package containing physical medical supplies

        --the claimed identification of the physical medical supplies; and

--the claimed transmitting the physical package to a remote site is met by the prescription

distribution system that enable quicker delivery of prescription at the patient's location (see:

abstract and column 5, lines 7-10); and

the received package data comprising:

identification of a physical package received by the remote site; identification of a patient

prescription received by the remote site; and

identification of the remote site;

--the claimed authorizing release of the physical package if the stored package data

identification of the at least one physical package matches the received package data

identification of the at least one physical package;

the stored package data identification of the physical medical supplies matches the

received package data identification of the patient prescription; and

the stored package data remote site matches the received package data identification of

the remote site.

Portwood et al. teach a prescription distribution system including a server computer

communicating with other prescriber computer to transfer prescription data to the server for

validation, certification, and distribution (see: abstract, column 3, lines 43-49, column 5, lines 7-

10 and column 7, lines 35-37). In addition, Portwood et al. teaches that prescription can be

distributed to a prescription distribution company, such as a pharmacy, or drug wholesale

company, and in turn the distribution can, via the server, invoice the payor (see: column 7, lines

42-45). The Examiner considers the invoice to contain patient identification information and site

information.

Portwood et al. fails to teach the claimed receiving the package data from the remote site.

Evans teaches a system for instant access to a patient's electronic medical record from any geographical location and the transferring and receiving patient record external sources (see: column 2, lines 45-47 and column 10, lines 18-23).

Therefore, it would have been obvious to one having ordinary skill in the art at the time of the invention to include the electronic medical record system as taught by Evans with the prescription distribution system as taught by Portwood et al. with the motivation of streamlining and incorporating automatic mail ordering, billing, and other business aspects, such as prescription verification and delivery (see: Portwood et al. column 2, lines 9-13).

As per claim 21, Portwood et al. teaches the claimed generating patient counseling data. This limitation is met by the prescription message that includes instruction on how to take the medication or how to conduct various medical procedures (see: column 17, lines 17-22).

As per claim 22, Portwood et al. teaches the claimed incrementing order data after the package is released is met by the ordering of prescription refills which enable the system to keep track to increase or decrease a refill of a patient prescription (see: column 2, lines 44-47).

8.   Claims 25-26 and 32 are rejected under 35 U.S.C. 103(a) as being unpatentable over U.S. Patent No. 5,924,074 to Evans.

As per claims 25-26, Evans teaches the transfer of patient data from the electronic medical records system to other healthcare providers as well as the updating of patient's record upon a nurses or physician entry of information into the system (see: column 4, lines 64 to column 5, lines 8, column 3, lines 36-42 and column 5, lines 29-40). In addition, Evans further

teaches a tiered password system to ensure patient confidentiality and provides several levels of

security for access to patient data (see: column 15, lines 9-32).

Although Evans fails to teach the remote system operates in an unattended mode that

allows the electronic medical data to be transferred without operator input. Evans teaches that

information is updated and transferred upon input by an authorized and the Examiner considers

the feature of transferring data in an unattended mode to be merely automatically updating or

transferring the data without an operator inputs and an old and well-known feature in the art.

Therefore, it would have been obvious to a person of ordinary skill in the art to include

automatically updating or transferring data without an operator inputs within the system as

taught by Evans with the motivation of providing an up-to-date medical record to authorized

personnel to better treat the patient.

As per claim 32, it is rejected for the same reasons set forth in claims 25-26.

9.   Claim 34 is rejected under 35 U.S.C. 103(a) as being unpatentable over U.S. Patent No.

5,924,074 to Evans and U.S. Patent No. 6,305,377 to Portwood et al. in view U.S. Patent No.

6,370,841 to Chudy et al.

As per claim 34, Evans and Portwood et al. teach a record server and record client

coupled to the record server (see: Evans: column 14, lines 8-16).

Evans and Portwood et al. fails to teach a data reader configured to read verification data

from a package.

Chudy et al. teaches automated method for dispensing bulk medication that uses scanner

device (129) for transmitting scanned code to the computer (119, Fig. 25) and generating a signal

for computer (119, Fig. 25) to confirm that the package correspond to the patient's drug

prescription information (see: column 14, lines 54-63).

One of ordinary skill in the art at the time the invention was made would have found it

obvious to include the scanner device for reading and transmitting prescription information as

taught by Chudy et al. within the electronic medical record system as taught by Evans with the

motivation of storing a broad range of prescription information and the ability to fill patient

prescription in rapid and efficient manner (see: column 1, lines 31-33).

Response to Arguments

Applicant's arguments filed 7/28/09 have been fully considered but they are not

persuasive. Applicant's arguments will be addressed hereinbelow in the order in which they

appear in the response 7/28/09.

With regard to Applicant's arguments, it is respectfully submitted that the Examiner has

applied recited new passages and citations to amended claims 1, 3, 7, 9-13, 15-17, 20, 23-24, 27,

and 29 and newly added claim 36 at the present time. The Examiner notes that the amended and

newly added limitations were not in the previously pending claims as such, Applicant's remarks

with regard to the application of Evans, Nichols, Portwood et al. and/or Chudy et al. to the

amended limitations are moot in light of Alban et al. reference and addressed in the above Office

Action.

Conclusion

Any inquiry concerning this communication or earlier communications from the

examiner should be directed to ROBERT W. MORGAN whose telephone number is (571)272-

6773. The examiner can normally be reached on 9:00 a.m. - 5:30 p.m. Mon - Fri.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, C. Luke Gilligan can be reached on (571) 272-6770. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/Robert Morgan/
Primary Examiner, Art Unit 3626